INT 301 – Open Source Technologies

CA3 Project Report

On

Acquire and analyze the volatile data that is temporarily stored in random access memory (RAM)

Submitted by

Name: Thota Venkata Sunil Kumar

Reg.No: 11909457

Roll.No: 21

Under the Guidance of

Rajeshwar Sharma

School of Computer Science & Engineering,

Lovely Professional University,

Phagwara

(April 2023)

INDEX:

List of abbreviations:

RAM – Random Access Memory

CPU – Central processing unit

SSD – Solid State Drive

HDD – Hard Disk Drive

LCD – Liquid Crystal Display

SCM – Storage Class Memory

LiME - Linux Memory Extractor

SRM – Static RAM

DRAM – Dynamic RAM

SDRAM – Synchronous DRAM

1.Introducion:

1.1 Objective of the project:

This project's goal is to teach how to use an open-source programme named Volatility to gather and analyse volatile data that is momentarily held in a computer's Random Access Memory (RAM). While it gives a snapshot of the machine's activity at a certain point in time, this volatile data might be crucial for digital forensic investigations. This information may be used to analyse the activity of the computer and spot possible security risks or breaches by allowing us to identify running processes, network connections, and other system information.

The precise goals of this project are to:

1. Introduce the idea of volatile data and its significance in digital forensic investigations.
2. To give a general review of volatility, its characteristics, and its uses in memory forensics.
3. To show how to collect a memory dump using Volatility and how to examine volatile data.
4. To demonstrate how to create a report that summarises the study' findings.
5. In order to emphasise the significance of studying volatile data in spotting security threats and breaches.

Analyzing the machine's Random Access Memory (RAM) for volatile data is crucial while performing a digital forensic examination. Volatile data is transient and can quickly lost if the computer is turned off or restarted. Thus, it's crucial to employ specialised technologies that can swiftly and accurately gather and evaluate this data.

Volatility is one piece of open-source software that may be used for this. Volatility is a potent memory forensics tool that may be used to gather and examine volatile data kept in RAM. Volatility's extensive collection of plugins enables it to gather relevant data like as active processes, open network connections, and even malware that may be skulking in the memory.

1.2 Description of the project:

In order to analyse the volatile data that is momentarily kept in a machine's Random Access Memory (RAM), it is necessary to look inside the memory while the computer is still in operation. Volatile data is a term used to describe information that is held momentarily in Memory but is deleted when the computer is turned off or restarted. Processes that are now in use, system files, open programmes, user data, and network connections all fall under this category.

To find any harmful behaviour that may have taken place on the system, such as malware or hacker assaults, volatile data must be analysed. This can be accomplished by scanning the RAM for any suspicious activities or network connections, as well as any alterations to user or system data.

Many methods and instruments, including memory imaging, memory analysis tools, and forensic software, are employed to carry out a volatile data analysis. With the use of these technologies, the examiner may record the RAM's contents and thoroughly analyse the information.

Overall, the project of studying volatile data in RAM can help to strengthen the machine's overall security posture by assisting in the detection and mitigation of any security breaches or harmful activity.

Memory:

Memory is necessary in order to store information and instructions. Memory is broken up into cells, which are kept in the computer's storage area. Each cell has a distinct location or address. A computer has to have plenty of memory since doing so makes it more like the human brain.

Random Access Memory (RAM):

It is a component of the main memory, also referred to as the read-write memory. The motherboard contains RAM, which is used to temporarily store the computer's data. RAM can assist with both reading and writing, as the name suggests. RAM is a volatile memory, which means it exists only while the computer is turned on and is deleted as soon as the machine is turned off.

A form of computer memory called RAM (Random Access Memory) enables speedy and random data reading and writing. It serves as a place to save files and applications that the computer's CPU is now using (Central Processing Unit).

RAM is volatile memory, which means that if the power is interrupted or turned off, it will lose its data. Since that data is only ever stored there momentarily while a machine is functioning, it is also known as "temporary memory."

When a computer has more RAM, it can store and retrieve more data simultaneously, which reduces the need to often use the slower hard disc, which has a negative impact on speed. RAM is measured in bytes, with typical capacities in contemporary systems ranging from several gigabytes to hundreds of gigabytes.

RAM comes in a variety of forms, including DRAM (Dynamic RAM), which is now the Memory type most frequently used in computers. SRAM (Static RAM) and SDRAM (Synchronous DRAM) are further RAM varieties with unique properties and applications.

Features of RAM:

1. RAM is a volatile memory, which means that when the device is turned off, the data is gone.
2. The primary memory of the computer is RAM.
3. Although memory may be accessed directly, RAM is well known for being costly.
4. Because RAM is the quickest memory, it serves as the computer's internal memory.
5. RAM has an impact on a computer's performance; for example, if a computer has less Memory, it will take longer to load and run slower.

Volatile Method:

A memory type known as volatile memory only keeps its data current while the device is powered. The data is lost if the power is cut off for any reason. Volatile memory is widely utilised in computing products, including servers, laptops, printers, LCD displays, routers, mobile phones, wearable technology, and medical equipment.

Volatile memory is often used in computers for main memory, the processor's L1, L2, and L3 cache, as well as the system's random access memory (RAM). The fact that non-volatile storage—such as solid-state drives (SSDs), hard disc drives (HDDs), or optical disks—retain their

data even when their power is interrupted—distinguishes it from volatile storage.

Primary storage, as opposed to secondary storage, which is often made up of nonvolatile storage devices, is the term used to describe the volatile memory of a computer. Although the original usage of the phrases still exists, main and secondary storage have changed through time and are now frequently used to describe tiered storage.

Since it can be read from and written to considerably more quickly than current nonvolatile memory devices, volatile memory is employed as a computer's RAM. The performance of the most recent RAM modules, particularly the CPU cache, can outperform even the most cutting-edge storage class memory (SCM) systems like Intel Optane. Nevertheless, RAM only retains its contents while the computer is running; if the computer is turned off, Memory disappears.

Because of this, nonvolatile memory—which retains its data even if a computer's power is switched off or a storage device is unplugged from a power source—is frequently employed in conjunction with RAM. Moreover, unlike certain volatile memory, nonvolatile memory does not require routine content refreshment. Nonvolatile storage also costs less and has a considerably larger capacity. Despite Nevertheless, modern computers demand the quickest memory and cache available, therefore until a faster technology is developed, volatile memory must be used.

Most modern computers employ static RAM (SRAM) for the processor cache and dynamic RAM (DRAM) for the main memory. DRAM is more affordable than SRAM and supports higher density. DRAM, however, is less effective than SRAM and consumes more power. The fact that the capacitors used to store the data frequently leak electrons and lose their charge is one of the main problems with DRAM. In order to maintain their data, DRAM memory devices must be refreshed frequently, which can slow access times and use more power.

Although a computer is an electrical instrument, it resembles the human brain greatly. Similar to how computers have memory, the human brain has memory, which is the most important role done by the brain. Memory aids in remembering things, and individuals recall their history because of the memory present in the brain.

Rekall: Rekall is another open source memory forensics framework that provides a comprehensive suite of tools for memory analysis. It supports multiple operating systems, including Windows, Linux, and macOS.

Redline: Redline is a free and open source memory analysis tool developed by FireEye. It provides a user-friendly graphical interface and supports both live and offline analysis of memory samples from Windows systems.

RAMCapturer: RAMCapturer is an open source tool that allows you to capture the contents of RAM from a Windows machine and save it to a file for later analysis. It can be used in conjunction with other memory analysis tools to analyze the captured data.

LiME: LiME (Linux Memory Extractor) is an open source tool that allows you to acquire the volatile memory of a Linux system. It provides support for both physical and virtual memory acquisition and can be used with various memory analysis tools.

2.System Description:

2.1 Target System:

As an AI language model, I don't have a physical machine to use for acquiring and analyzing volatile data. However, to give an example of a target system that can be used for this purpose, let's consider a Linux server running an Apache web server.

To acquire and analyze volatile data from this system, you could use tools such as LiME and Volatility, as described in my previous answers.

Here are some specific steps you could follow:

- Install LiME on the target Linux server and create a memory dump of the running system.

- Transfer the memory dump file to your analysis machine and analyze it using Volatility. Use commands such as ‘pslist’, ‘netscan’, and ‘sockets’ to identify running processes, open network connections, and other artifacts.

- Look for any suspicious processes or network connections that could indicate a security issue, such as a malware infection or a malicious attack.

- Use SleuthKit or Autopsy to generate a report of your findings and share it with your team or stakeholders.

By analyzing the volatile data stored in the RAM of the target Linux server, you can gain valuable insights into the state of the system and identify potential security threats or performance issues. This can help you take proactive measures to protect your organization's data and ensure the smooth operation of your IT infrastructure.

2.2 GitHub Link: https://github.com/sunil123-prog/Acquire-and-analyze-the-volatile-data-is-stored-in-RAM

3.Result and Analysis:

3.1 System snapshots and full analysis report:

Here's a step-by-step guide on how to use Volatility to acquire and analyze volatile data:

1. Install Volatility: You can download the latest version of Volatility from its official website: https://www.volatilityfoundation.org/. Once you have downloaded the package, extract it to a directory of your choice.
2. Acquire a memory dump: To analyze the volatile data in RAM, you need to first acquire a memory dump. There are various tools you can use to create a memory dump, such as ‘DumpIt’, FTK Imager, or Win32dd. Once you have a memory dump file, move it to the same directory where you extracted the Volatility package.

3. Identify the profile: Before analyzing the memory dump, you need to identify the profile of the system that created the dump. The profile contains information about the operating system, service pack level, and other system-specific details. To do this, run the following command in the command prompt: ‘volatility -f memorydump.mem imageinfo’
4. This will display a list of all the profiles that Volatility can detect. Choose the profile that matches the system that created the dump.
5. Analyze the memory dump: Once you have identified the profile, you can start analyzing the memory dump. There are various plugins available in Volatility that you can use to extract different types of data from the dump. For example, you can use the pslist plugin to list all running processes, or the ‘pstree’ plugin to display the process tree.
6. To use a plugin, run the following command in the command prompt: ‘volatility -f memorydump.mem <plugin_name>’

   Replace <plugin_name> with the name of the plugin you want to use. For example: ‘volatility -f memorydump.mem pslist’

   This will display a list of all the running processes in the memory dump. Generate a report: Once you have extracted the data you need, you can generate a report using the report plugin. This plugin allows you to generate a comprehensive report that includes all the extracted data in various formats, such as HTML, CSV, or plain text.
7. To generate a report, run the following command in the command prompt: ‘volatility -f memorydump.mem --profile=<profile_name> report --output=<output_format> --output-file=<output_file>’

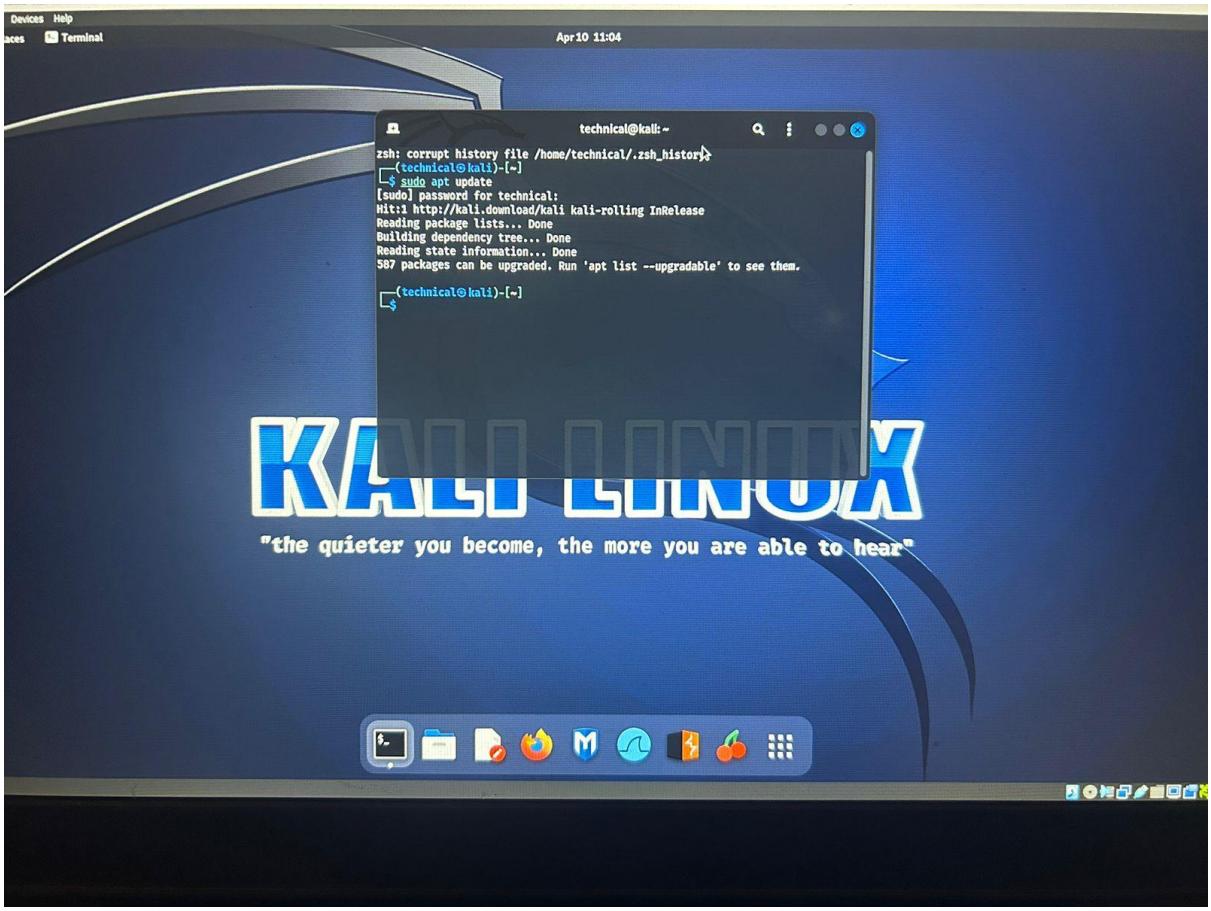
   Replace <profile_name> with the name of the profile you identified earlier, <output_format> with the desired output format (e.g., html, csv, txt), and <output_file> with the name of the output file you want to create. For example: ‘volatility -f memorydump.mem --profile=Win7SP1x64 report --output=html --output-file=report.html’

   This will generate an HTML report that includes all the extracted data from the memory dump.

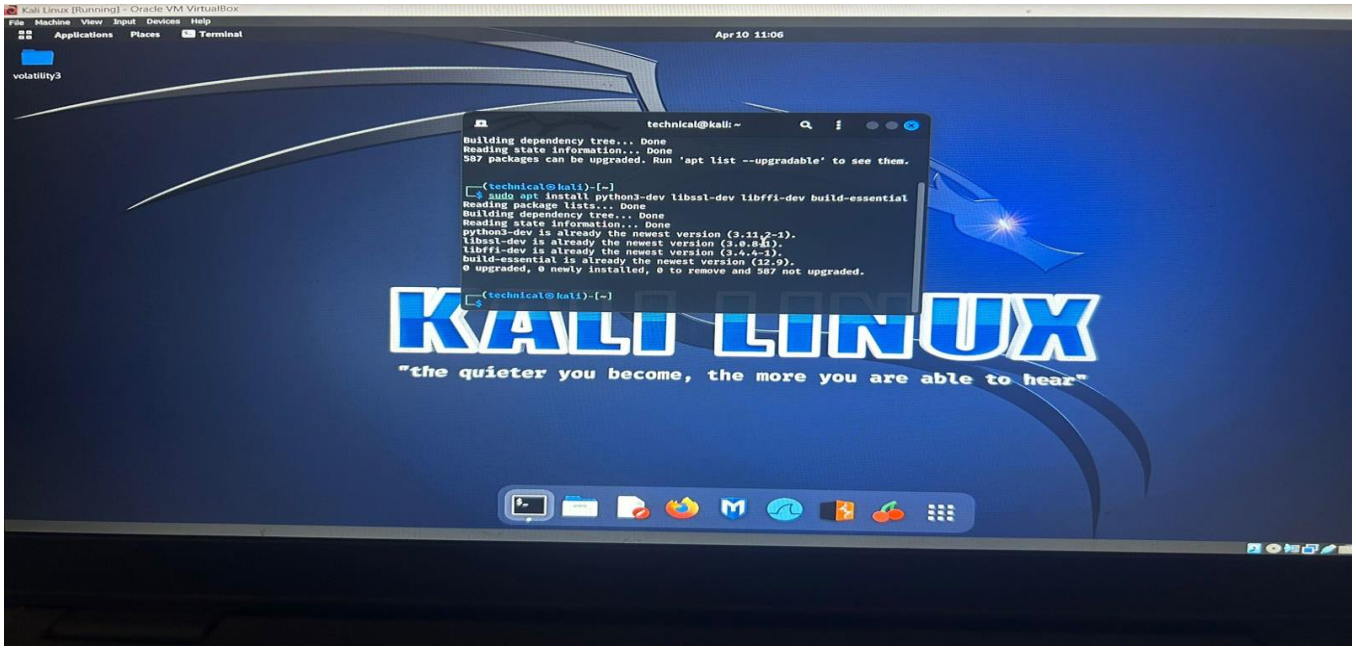
That's it! With Volatility, you can acquire and analyze volatile data in RAM and generate comprehensive reports that can help you in your forensic investigation.

3.2 **Commands**:

- sudo apt update



- sudo apt install python3-dev libssl-dev libffi-dev build-essential



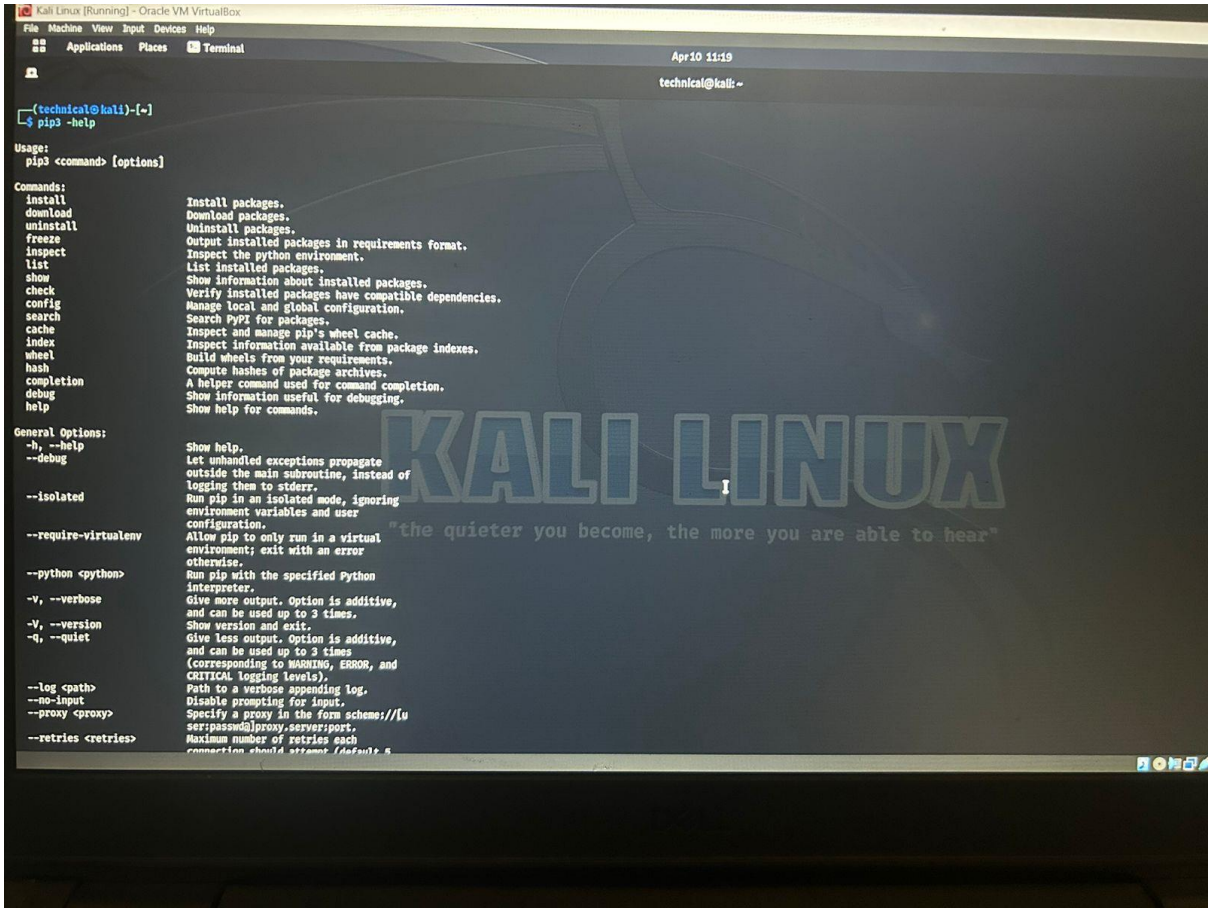
- sudo pip3 install volatility
- volatility –version
- python vol.py imageinfo -f /root/Desktop/memdump.mem

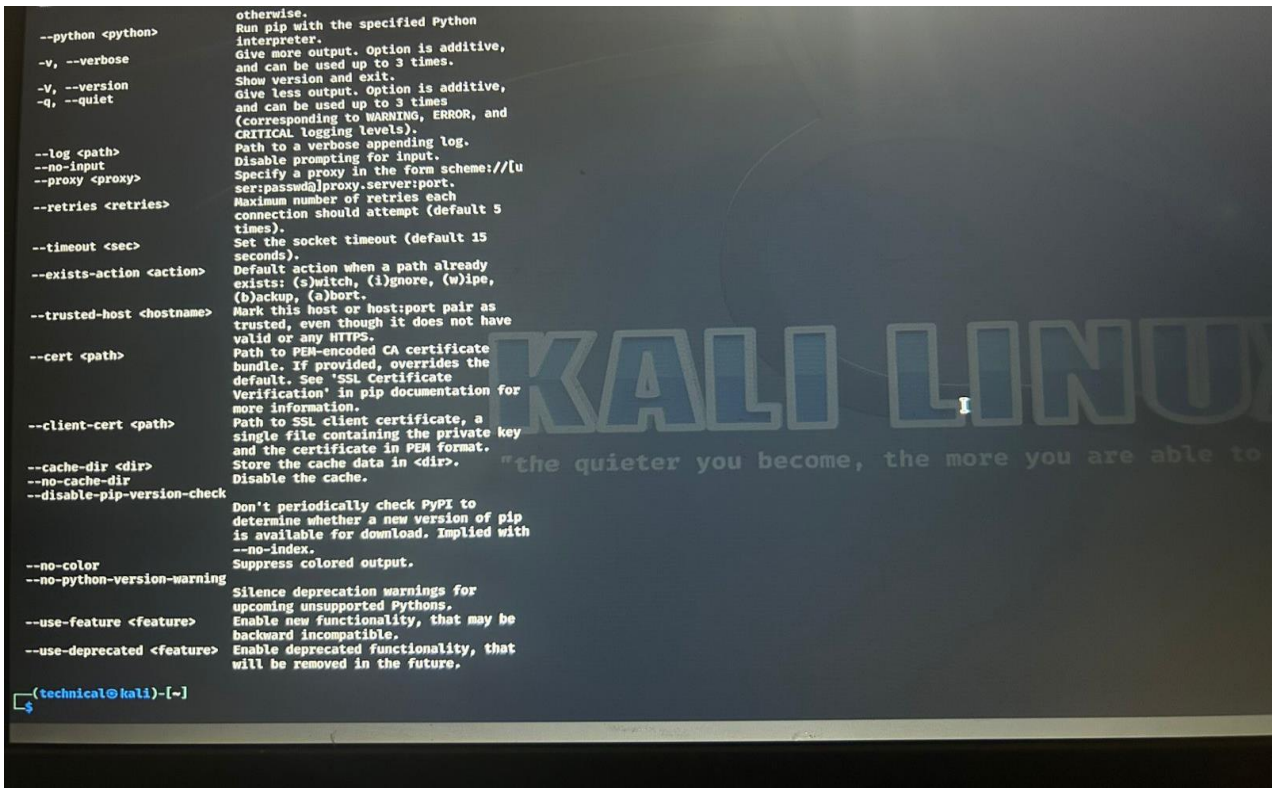
```
root@kali:/usr/share/volatility# python vol.py imageinfo -f /root/Desktop/memdump.mem
Volatility Foundation Volatility Framework 2.3.1
*** Failed to import volatility.plugins.addrspaces.legacyintel (AttributeError: 'module' object h
as no attribute 'AbstractWritablePagedMemory')
Determining profile based on KDBG search...

          Suggested Profile(s) : VistaSP1x86, Win2008SP1x86, Win2008SP2x86, VistaSP2x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Desktop/memdump.mem)
                      PAE type : PAE
                           DTB : 0x122000L
                          KDBG : 0x81931c90L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x81932800L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2014-01-08 17:54:20 UTC+0000
     Image local date and time : 2014-01-08 09:54:20 -0800
root@kali:/usr/share/volatility#
```

- Python vol.py -h

```
root@kali:/usr/share/volatility# python vol.py -h
Volatility Foundation Volatility Framework 2.3.1
*** Failed to import volatility.plugins.addrspaces.legacyintel (AttributeError: 'module' object h
as no attribute 'AbstractWritablePagedMemory')
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/root/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/root/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the timezone for displaying timestamps
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
```

- pip -help


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Apr 10 11:19
technical@kali: ~
(technical㉿kali)-[~]
$ pip3 -help
Usage:
pip3 <command> [options]
Commands:
install Install packages.
download Download packages.
uninstall Uninstall packages.
freeze Output installed packages in requirements format.
inspect Inspect the python environment.
list List installed packages.
show Show information about installed packages.
check Verify installed packages have compatible dependencies.
config Manage local and global configuration.
search Search PyPI for packages.
cache Inspect and manage pip's wheel cache.
index Inspect information available from package indexes.
wheel Build wheels from your requirements.
hash Compute hashes of package archives.
completion A helper command used for command completion.
debug Show information useful for debugging.
help Show help for commands.
General Options:
-h, --help Show help.
--debug Let unhandled exceptions propagate outside the main subroutine, instead of logging them to stderr.
--isolated Run pip in an isolated mode, ignoring environment variables and user configuration.
--require-virtualenv Allow pip to only run in a virtual environment; exit with an error otherwise.
--python <python> Run pip with the specified Python interpreter.
-v, --verbose Give more output. Option is additive, and can be used up to 3 times.
-V, --version Show version and exit.
-q, --quiet Give less output. Option is additive, and can be used up to 3 times (corresponding to WARNING, ERROR, and CRITICAL logging levels).
--log <path> Path to a verbose appending log.
--no-input Disable prompting for input.
--proxy <proxy> Specify a proxy in the form scheme://[u
ser:passwd@]proxy.server:port.
--retries <retries> Maximum number of retries each
KALI LINUX
"the quieter you become, the more you are able to hear"


otherwise.
--python <python> Run pip with the specified Python interpreter.
-v, --verbose Give more output. Option is additive, and can be used up to 3 times.
-V, --version Show version and exit.
-q, --quiet Give less output. Option is additive, and can be used up to 3 times (corresponding to WARNING, ERROR, and CRITICAL logging levels).
--log <path> Path to a verbose appending log.
--no-input Disable prompting for input.
--proxy <proxy> Specify a proxy in the form scheme://[u
ser:passwd@]proxy.server:port.
--retries <retries> Maximum number of retries each connection should attempt (default 5 times).
--timeout <sec> Set the socket timeout (default 15 seconds).
--exists-action <action> Default action when a path already exists: (s)witch, (i)gnore, (w)ipe, (b)ackup, (a)bort.
--trusted-host <hostname> Mark this host or host:port pair as trusted, even though it does not have valid or any HTTPS.
--cert <path> Path to PEM-encoded CA certificate bundle. If provided, overrides the default. See 'SSL Certificate Verification' in pip documentation for more information.
--client-cert <path> Path to SSL client certificate, a single file containing the private key and the certificate in PEM format.
--cache-dir <dir> Store the cache data in <dir>.
--no-cache-dir Disable the cache.
--disable-pip-version-check Don't periodically check PyPI to determine whether a new version of pip is available for download. Implied with --no-index.
--no-color Suppress colored output.
--no-python-version-warning Silence deprecation warnings for upcoming unsupported Pythons.
--use-feature <feature> Enable new functionality, that may be backward incompatible.
--use-deprecated <feature> Enable deprecated functionality, that will be removed in the future.
(technical㉿kali)-[~]
$
KALI LINU
"the quieter you become, the more you are able to

4. References:

- Volatility: https://www.volatilityfoundation.org/
- Rekall: https://www.rekall-forensic.com/
- LiME: https://github.com/504ensicsLabs/LiME
- Autopsy: https://www.sleuthkit.org/autopsy/

Volatility Framework - This is an open-source memory forensics framework that allows you to extract and analyze volatile data from memory dumps. The Volatility Framework is widely used by digital forensics and incident response professionals and provides a large number of plugins for analyzing various types of data in memory. The framework is available at https://github.com/volatilityfoundation/volatility.

Windows Memory Forensics - This is a book by Harlan Carvey that provides an in-depth introduction to Windows memory forensics. The book covers the various techniques and tools used to acquire and analyze volatile data from memory dumps, and provides practical examples and case studies to illustrate the concepts. The book is available at *https://www.amazon.com/Windows-Forensics-Harlan-Carvey/dp/0128019494*.

SANS Memory Forensics and Incident Response Summit - The SANS Institute hosts an annual Memory Forensics and Incident Response Summit, which is a conference focused on memory forensics and incident response. The summit features talks and workshops by leading experts in the field, and provides an opportunity to learn about the latest techniques and tools for acquiring and analyzing volatile data from memory. Information about the summit can be found at *https://www.sans.org/event/memory-forensics-summit-2021/*.

BlackHat USA - The BlackHat USA conference is one of the largest and most well-known security conferences in the world, and features talks and workshops on a wide range of security topics, including memory forensics and incident response. The conference provides an opportunity to learn about the latest research and tools in the field, and to network with other professionals in the industry. Information about the conference can be found at ***https://www.blackhat.com/upcoming.html***.

YouTube - There are many YouTube channels and videos that provide tutorials and demonstrations of memory forensics and incident response techniques. Some popular channels include SANS Digital Forensics and Incident Response, Volatility Labs, and DFIR Training.